Dot1x로 Flexconnect AP 스위치 포트 보안

목차

소개

이 문서에서는 FlexConnect 액세스 포인트(AP)가 device-traffic-class=switch Radius VSA를 사용하여 Dot1x로 인증하여 로컬로 스위칭된 WLAN(무선 LAN)에서 트래픽을 허용하는 스위치 포트를 보호하는 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WLC(Wireless Lan Controller)의 FlexConnect
- Cisco 스위치의 802.1x
- NEAT(Network Edge Authentication Topology)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

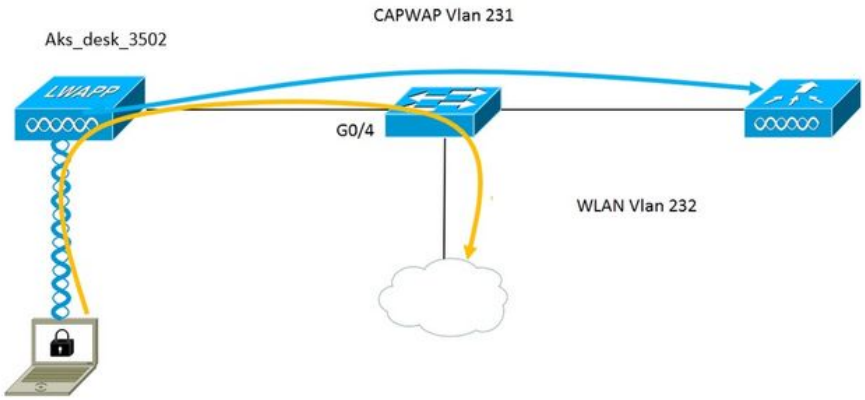
- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- ISE(Identity Service Engine) 2.0
- IOS 기반 액세스 포인트(x500,x600,x700 시리즈).

AP OS를 기반으로 하는 Wave 2 AP는 이 쓰기 시점부터 flexconnect trunk dot1x를 지원하지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

네트워크 다이어그램



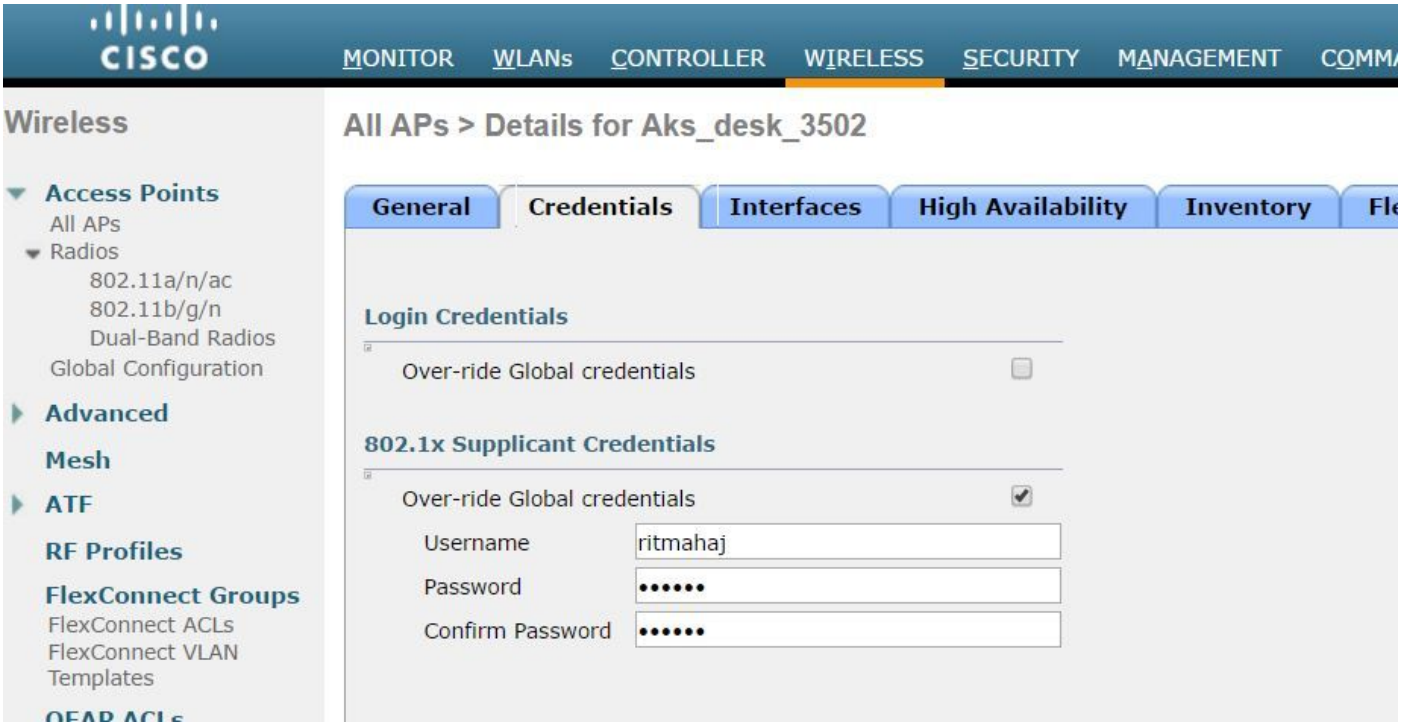
이 설정에서 액세스 포인트는 802.1x 신청자 역할을 하며 EAP-FAST를 사용하여 ISE에 대해 스위치에 의해 인증됩니다. 포트가 802.1x 인증을 위해 구성되면, 스위치에 연결된 디바이스가 성공적으로 인증될 때까지 스위치는 802.1x 트래픽 이외의 트래픽이 포트를 통과하도록 허용하지 않습니다.

액세스 포인트가 ISE에 대해 성공적으로 인증되면 스위치는 Cisco VSA 특성 "device-traffic-class=switch를 수신하고 자동으로 포트를 트렁크로 이동합니다.

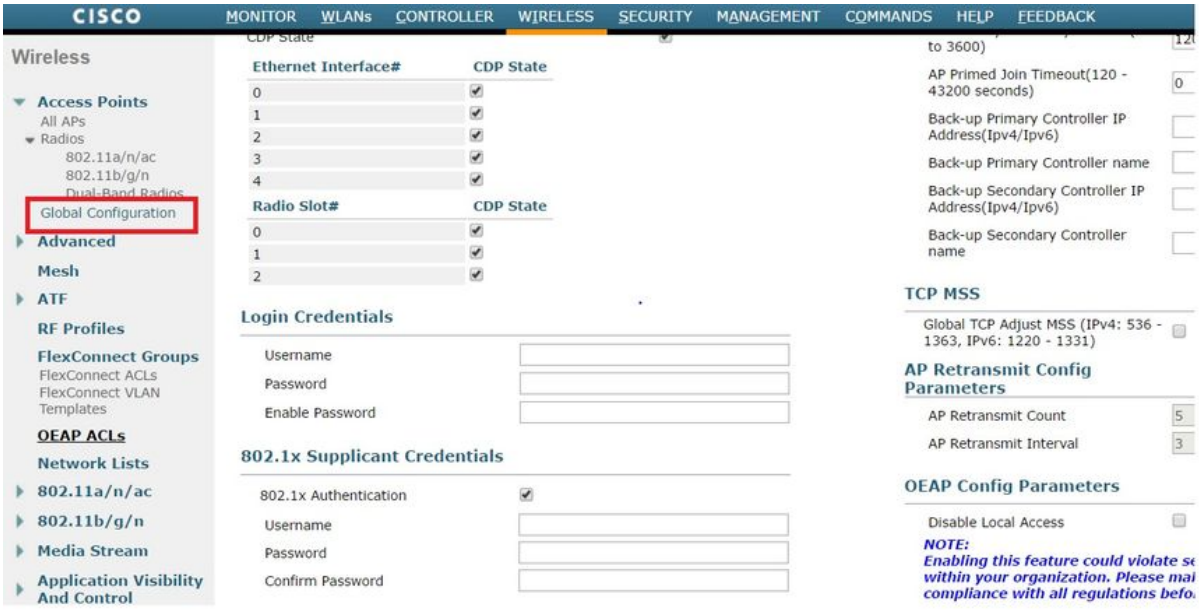
즉, AP가 FlexConnect 모드를 지원하고 로컬로 스위칭된 SSID를 구성한 경우 태그 처리된 트래픽을 전송할 수 있습니다. AP에서 VLAN 지원이 활성화되고 올바른 네이티브 VLAN이 구성되었는지 확인합니다.

AP 컨피그레이션:-

1. AP가 이미 WLC에 가입되어 있으면 Wireless(무선) 탭으로 이동하여 액세스 포인트를 클릭합니다. Credentials(자격 증명) 필드로 이동하여 802.1x Supplicant Credentials(802.1x 신청자 자격 증명) 머리글 아래에서 Over-**Ride Global credentials(오버라이드 전역 자격 증명**) 상자를 선택하여 이 액세스 포인트의 802.1x 사용자 이름과 비밀번호를 설정합니다.



또한 Global Configuration(전역 컨피그레이션) 메뉴를 사용하여 WLC에 연결된 모든 액세스 포인트에 대해 공통 사용자 이름과 비밀번호를 설정할 수 있습니다.



2. 액세스 포인트가 아직 WLC에 가입하지 않은 경우 LAP에 콘솔하여 자격 증명을 설정하고 다음 CLI 명령을 사용해야 합니다.

LAP#debug capwap 콘솔 cli
LAP#capwap ap dot1x username <username> password <password>

스위치 구성:-

1. 스위치에서 dot1x를 전역적으로 활성화하고 스위치에 ISE 서버를 추가합니다.

aaa 새 모델

!
aaa 인증 dot1x 기본 그룹 반경

!
aaa 권한 부여 네트워크 기본 그룹 radius

!

dot1x 시스템 인증 제어

!

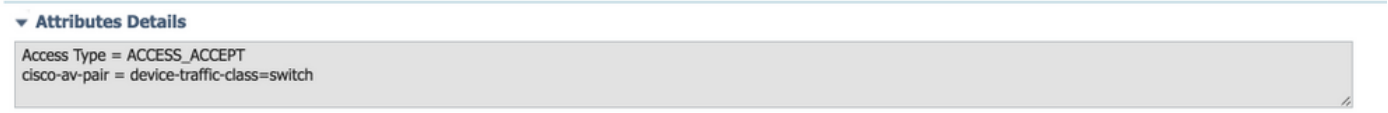
radius 서버 ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
 키 7 123A0C0411045D5679

2. 이제 AP 스위치 포트를 구성합니다.

인터페이스 GigabitEthernet0/4
switchport access vlan 231
switchport trunk allowed vlan 231,232
스위치 포트 모드 액세스
인증 호스트 모드 다중 호스트
인증 순서 dot1x
인증 포트 제어 자동
dot1x 인증자
스패닝 트리 포트 에지

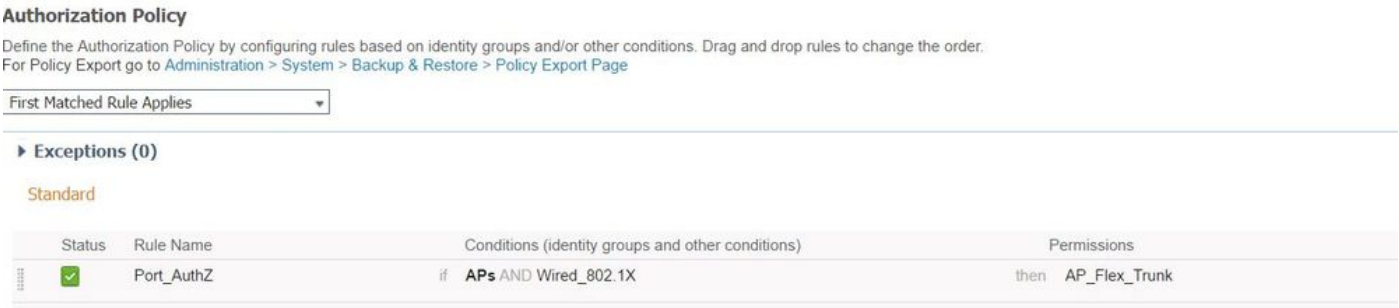
ISE 구성:-

1. ISE에서 AP 권한 부여 프로파일에 대해 NEAT를 활성화하면 올바른 특성을 설정할 수 있지만 다른 RADIUS 서버에서 수동으로 구성할 수 있습니다.



2. ISE에서 인증 정책 및 권한 부여 정책을 구성해야 합니다. 이 경우 유선 dot1x인 기본 인증 규칙을 실행했지만 요구 사항에 따라 사용자 지정할 수 있습니다.

권한 부여 정책(Port_AuthZ)에 대해 이 경우 AP 자격 증명을 사용자 그룹(AP)에 추가하고 이를 기반으로 권한 부여 프로파일(AP_Flex_Trunk)을 푸시했습니다.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

1. 스위치에서 "debug authentication feature autoconfig all" 명령을 사용하여 포트가 트렁크 포트로 이동되는지 여부를 확인할 수 있습니다.

2월 20일 12:34:18.119: %LINK-3-업다운: 인터페이스 GigabitEthernet0/4, 상태가 up으로 변경됨
2월 20일 12:34:19.122: %LINEPROTO-5-업다운: 인터페이스 GigabitEthernet0/4의 회선 프로토콜, 상태가 up으로 변경됨
akshat_sw#
akshat_sw#
2월 20일 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: dot1x AutoCfg start_fn, epm_handle에서 다음을 수행합니다. 3372220456
2월 20일 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] 장치 유형 = 스위치
2월 20일 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] 새 클라이언트
2월 20일 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] 내부 Autofg 매크로 응용 프로그램 상태: 1
2월 20일 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] 장치 유형: 2
2월 20일 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] 자동 구성: stp에 port_config 0x85777D8 포함
2월 20일 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] 자동 구성: stp port_config에 bpdu guard_config 2가 있습니다.
2월 20일 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] 포트에 auto-cfg를 적용합니다.
2월 20일 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] VLAN: 231 VLAN-Str: 231
2월 20일 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] dot1x_autocfg_supp 매크로 적용
2월 20일 12:38:11.116: 명령을 적용하는 중... Gi0/4에서 'no switchport access vlan 231'
2월 20일 12:38:11.127: 명령을 적용하는 중... Gi0/4에서 'switchport nonegotiate' 없음
2월 20일 12:38:11.127: 명령을 적용하는 중... Gi0/4에서 'switchport mode trunk'
2월 20일 12:38:11.134: 명령을 적용하는 중... Gi0/4에서 'switchport trunk native vlan 231'
2월 20일 12:38:11.134: 명령을 적용하는 중... Gi0/4에서 'spanning-tree portfast trunk'
2월 20일 12:38:12.120: %LINEPROTO-5-업다운: Interface GigabitEthernet0/4의 회선 프로토콜,

상태가 down으로 변경됨
2월 20일 12:38:15.139: %LINEPROTO-5-업다운: 인터페이스 GigabitEthernet0/4의 회선 프로토콜, 상태가 up으로 변경됨

2. "show run int g0/4"의 출력에는 포트가 트렁크 포트로 변경되었음을 나타냅니다.

현재 구성: 295바이트
!
인터페이스 GigabitEthernet0/4
switchport trunk allowed vlan 231,232,239
switchport trunk native vlan 231
스위치 포트 모드 트렁크
인증 호스트 모드 다중 호스트
인증 순서 dot1x
인증 포트 제어 자동
dot1x 인증자
스패닝 트리 포트 에지 트렁크
끝

3. ISE의 Operations(작업) > Radius Livelogs 아래에서 인증 성공 및 푸시되는 올바른 권한 부여 프로파일을 확인할 수 있습니다.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
	All								
2017-02-20 15:05:48.991			0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:05:48.991				ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:04:49.272				ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	

4. 이 이후에 클라이언트를 연결하면 해당 mac 주소가 클라이언트 vlan 232의 AP 스위치 포트에서 학습됩니다.

akshat_sw#sh mac 주소 테이블 int g0/4
MAC 주소 테이블
—

VLAN MAC 주소 유형 포트
— — — — — —
231 588d.0997.061d 고정 Gi0/4 - AP
232 c0ee.fbd7.8824 DYNAMIC Gi0/4 - 클라이언트

WLC에서 클라이언트 세부사항에서 이 클라이언트가 vlan 232에 속하고 SSID가 로컬로 스위칭되는 것을 확인할 수 있습니다. 여기 코드 조각이 있습니다.

(Cisco Controller) >show client detail c0:ee:fb:d7:88:24
클라이언트 MAC 주소..... c0:ee:fb:d7:88:24
클라이언트 사용자 이름 ..... 해당 없음
AP MAC 주소..... b4:14:89:82:cb:90
AP 이름..... Aks_desk_3502
AP 무선 슬롯 ID.....1
클라이언트 상태..... 관련
클라이언트 사용자 그룹.....
클라이언트 NAC OOB 상태..... 액세스
무선 LAN ID.....2
무선 LAN 네트워크 이름(SSID)..... 포트 인증

무선 LAN 프로파일 이름..... 포트 인증
핫스팟(802.11u)..... 지원되지 않음
BSSID..... b4:14:89:82:cb:9f
연결 대상..... 42초
채널.....44
IP 주소..... 192.168.232.90
게이트웨이 주소..... 192.168.232.1
넷마스크..... 255.255.255.0
연결 ID..... 1
인증 알고리즘..... 오픈 시스템
이유 코드..... 1
상태 코드..... 0

FlexConnect 데이터 스위칭..... 로컬
FlexConnect DHCP 상태..... 로컬
FlexConnect VLAN 기반 중앙 스위칭..... 아니요
FlexConnect 인증..... 중앙
FlexConnect 중앙 연결..... 아니요
FlexConnect VLAN 이름..... vlan 232
VLAN 격리.....0
VLAN 액세스..... 232
로컬 브리징 VLAN.....232

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

- 인증이 실패하면 debug **dot1x**, debug **authentication** 명령**을** 사용합니다.
- 포트가 트렁크로 이동되지 않은 경우 debug **authentication feature autoconfig all** 명령**을** 입력합니다.
- 멀티호스트 모드(authentication host-mode multi-host)가 구성되어 있는지 확인합니다. 클라이언트 무선 MAC 주소를 허용하려면 멀티호스트를 활성화해야 합니다.
- 스위치가 ISE에서 보낸 특성을 수락하고 적용하려면 "aaa authorization network" 명령을 구성해야 합니다.

Cisco IOS 기반 액세스 포인트는 TLS 1.0만 지원합니다. RADIUS 서버가 TLS 1.2 802.1X 인증만 허용하도록 구성된 경우 문제가 발생할 수 있습니다.